REMARKS/ARGUMENTS

Claims 1-4, 8, 10-40, and 42-79 are pending. Claims 1-4, 8, 11, 13-18, 24, 25, 32-34, 39, 40, 42-46, 49, 51-55, 57, 60, and 72-73 are amended and claims 5-7, 9, and 41 are canceled.

Claims 1-79 are again rejected under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse** (US 6,005,945) in view of Pang (US 6,446,204). Applicant notes that the current Office action (mailed on March 13, 2007) is the **tenth Office action** received from the (same) Examiner, all of which cite **Whitehouse** as the primary reference. However, Applicant has repeatedly argued in detail that Whitehouse does not disclose a number of the limitations present in the independent and dependent claims. Applicant respectfully request that each and every one of the arguments articulated below, specially the ones regarding **Whitehouse** (including those with regard to dependent claims 5 and 6) be sufficiently addressed by the Examiner.

Amended independent claim 1 includes, among other limitations, "each transaction data record includes information to restore the data record to its last known state, when the data record is next used," "a plurality of stateless cryptographic devices remote from the client system and capable of authenticating and processing VBI printing requests from any of the plurality of users," and "wherein when a VBI printing request from a current user is received by the server system, an available cryptographic device from the plurality of cryptographic devices loads the current user's transaction data record and instantiates a user state in the transaction data record to process the VBI printing requests from the current user." Applicant respectfully submits that the combination of Whitehouse and Pang, alone or in combination does not teach or suggest the above limitations.

First, regarding the limitation of "each transaction data record includes information to restore the data record to its last known state, when the data record is next used," there is no teaching or suggestion in Whitehouse for this limitation. In fact, because each central computer 102 of Whitehouse stores the Customer Database 172 in its own local memory (RAM) 154 and the Customer Database 172 stores information about each of the user account received by [that particular] central computer (col. 8, lines 54-58, underlining added), each data record for each of

the users has already been stored in the local memory as the last known state and there is no restoring the data record to its last known state when the data record is next used." Similarly Pang, alone or in combination with Whitehouse, does not teach or suggest the above limitation.

Second, with regard to the limitation of "a plurality of cryptographic devices remote from the client system," Whitehouse does not have any cryptographic devices remote from the client system. Rather, there are Encryption Procedures 162 in the local memory 154 of Whitehouse's central computer 102. (Col. 8, lines 38-40 and FIG. 4, underlining added.). Also, see, col. 9, line 19: "encryption software and keys." Pang does not have any cryptographic devices either.

In contrast, the claimed invention includes a plurality of cryptographic devices in the server system. "Each of the cryptographic [devices] modules may be available for use by any user. When a user requests a PSD service, one of the available modules is loaded with data belonging to the user's account and the transaction is performed. When a module is loaded with a user's data, that module becomes the user's PSD. The database record containing each user's PSD data is referred to as the "PSD package" (security device transaction data). After each PSD transaction is completed, the user's PSD package is updated and returned to a database external to the module. The database becomes an extension of the module's memory. . ." (Page 7, lines 10-19, underlining added.). Additionally, "each cryptographic module is a stateless device, meaning that a PSD package can be passed to any device." (Page 8, lines 16-17, underlining added.).

Third, with respect to the limitation of "a plurality of cryptographic devices . . . capable of authenticating and processing VBI printing requests from any of the plurality of users," there is no teaching or suggestion in Whitehouse for this limitation either. Rather, Whitehouse's central computers 102 are not capable of "authenticating and processing VBI printing requests from any of the plurality of users," because each central computer 102 of Whitehouse stores the Customer Database 172 and the Transaction Database 174 in its own local memory (RAM) 154 and the transaction database 174 stores records concerning each postage indicium generated by the secure central computer 102. (Col. 8, lines 54-62 and FIG. 4, underlining added.). Therefore, one skilled in the art of computer architecture would readily realize that with this

Whitehouse's system architecture, the central computers 102 cannot process any of the plurality of users," because the central computers do not have access to all users' information, some of which is stored in the local memories of the other central computers. For the same reasoning, in Whitehouse's central computers 102 environment, in which Customer Database 172 and the Transaction Database 174 are stored in each computer's own local memory (RAM) 154, a user can NOT be authenticated using any of the cryptographic devices (even assuming that a central computer with "encryption software" can be construed as a cryptographic device).

Moreover, **Pang**, alone or in combination with Whitehouse, does not teach or suggest "processing VBI printing requests from any of the plurality of users." Additionally, Pang , alone or in combination with Whitehouse, does not teach or suggest " authenticating . . . any of the plurality of users." Rather, the authentication engines 802, 804, and 806 of Pang do NOT perform the authentication function. Rather, it is the provider(s) that perform the authentication function. "Each provider provides a specific authentication function to restrict access to a particular cartridge. For example, a BASIC provider may be associated with the authentication host and used to restrict cartridge access to only those browser requests that are associated with a particular username and password pair Another example of a type of provider that may be associated with authentication host is an IP address provider. The IP address provider can be used to restrict cartridge access to only those browser requests that are associated with a particular IP address.. (Col. 20, lines 26-47, underlining added.).

Pang is very clear about which modules/devices perform the authentication function (that is, the providers, as explained above). Pang emphasizes that "[o]nce the providers have completed the authentication of the provider requests, they send response messages back to the authentication engine . . .. Upon receiving the response messages from the one or more providers, the authentication engine performs any necessary logical operations on the returned response messages. The authentication engine then notifies the dispatcher whether the browser request should be forwarded to the appropriate cartridge or that the sending browser should be notified that access was denied." (Col. 23, line 65 to col. 7, line 6, underlining added.).

Therefore, it is clear from the above that the authentication modules (that is, the providers) of Pang are not capable of authenticating any of the plurality of users, because the Providers that are responsible for authentication each perform "a specific authentication function to restrict access to a particular cartridge." For example, BASIC Provider, IP Provider, DOMAIN name Provider, etc..

Fourth, regarding the limitation of "wherein when a VBI printing request from a current user is received by the server system, an available cryptographic device from the plurality of cryptographic devices loads the current user's transaction data record and instantiates a user state in the transaction data record to process the VBI printing requests from the current user," there is no teaching or suggestion in Whitehouse for this limitation, because Whitehouse does not have an available cryptographic device from the plurality of cryptographic devices and also there is no instantiation of a user state in the data records of Whitehouse.

Furthermore, **Pang**, alone or in combination with Whitehouse, does not teach or suggest the above limitation, because there is no instantiation of a user state in the data records of Pang.

Fifth, Applicant still fails to see any **motivation to combine** Pang with Whitehouse. The Examiner states that it would have been obvious to one skilled in the art to modify Whitehouse's system to include Pang's stateless cryptographic modules "because this would have ensure [sic] that client would be properly authenticate [sic] whenever service is needed." Applicant respectfully disagrees.

First, as explained above, there is no stateless cryptographic devices in Whitehouse or Pang. Second, it is not possible, without major architectural changes and a major overhaul of the system of Whitehouse, as described above with respect to "third argument," to make the Whitehouse system a scalable system, as described by Pang. Third, even if one could make the Whitehouse system a "scalable" system the "scalable" client-server environment does not enhance the authentication process of the system of Whitehouse. In fact, by making the Whitehouse environment a "scalable environment" as defined by Pang, the system of Whitehouse becomes enhanced with respect to the authentication function, because multiple providers would be needed and multiple copies of the cryptographic keys need to be generated

and stored in the local memories of the Whitehouse's computers. Fourth, each of the Whitehouse and Pang references are **individually complete** and **functional in itself**, one skilled in the art of computer authentication would see no reason to add parts to any of them. For example, one skilled in the art of computer authentication would readily appreciate that adding the "scalable environment" of Pang will not enhance the authentication of Whitehouse system, because Whitehouse system is already using a central computer to authenticate its users.

In short, based on at least the above-mentioned **five arguments**, each of which deemed sufficient by itself, the independent **claim 1** is patentable over cited references.

Amended independent **claim 39** includes, among other limitations, "wherein each transaction data record includes information to restore the data record to its last known state, when the data record is next used," "receiving a VBI printing request from a current user," "loading the current user's transaction data record in the cryptographic device," and "instantiating a user state in the transaction data record to process the VBI printing requests from the current user" As discussed above, the combination of Whitehouse and Pang does not teach or suggest the above limitations. Consequently, claim 39 is also patentable over cited references.

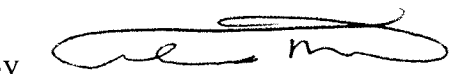
In short, independent claims 1 and 39 are patentable in view of the cited references. Dependent claims 2-4, 8, 10-38 and 48 and claims 42-47 and 49-79 depend from claims 1 and 39, respectively and include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested.

If the Examiner believes that a telephone conference would be useful in moving this application forward to allowance, the Examiner is encouraged to contact the undersigned at (626) 795-9900.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By 

Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS777879.1-*-02/11/08 2:46 PM